

ABSTRACT OF THE DISCLOSURE

An approach for managing addition or deletion of nodes in a multicast or broadcast group, which avoids introducing a single point of failure at a group controller, certificate authority, or key distribution center, is disclosed. A central group
5 controller utilizes a binary tree structure to generate and distribute session keys for the establishment of a secure multicast group among multiple user nodes. The central group controller is replicated in a plurality of other group controllers, interconnected in a network having a secure communication channel and connected to a load balancer. The secure communication channel is established using a public
10 key exchange protocol. The load balancer distributes incoming join/leave requests to a master group controller. The master group controller processes the join or leave, generates a new group session key, and distributes the new group session key to all other group controller replicas. Each group controller is successively designated as master group controller in real time when a former master group controller crashes or
15 relinquishes its master authority.